

The University of Chicago

COMPOSITION OF QUADRATIC FORMS

AN EXPANSION OF A DISSERTATION SUBMITTED TO THE
FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES IN
CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1943

By
ROY DUBISCH

Reprinted from
THE ANNALS OF MATHEMATICS
Vol. 47, No. 3, July, 1946

The University of Chicago

COMPOSITION OF QUADRATIC FORMS

AN EXPANSION OF A DISSERTATION SUBMITTED TO THE
FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES IN
CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1943

By
ROY DUBISCH



Reprinted from
THE ANNALS OF MATHEMATICS
Vol. 47, No. 3, July, 1946

COMPOSITION OF QUADRATIC FORMS

By ROY DUBISCH¹

(Received January 15, 1945)

(Revised November 14, 1945)

I. INTRODUCTION

Let $x_1, \dots, x_n, u_1, \dots, u_m$ be independent indeterminates over a field $\mathfrak{F}$ of characteristic not two, $\mathfrak{S} = \mathfrak{F}(x_1, \dots, x_n, u_1, \dots, u_m)$ be the corresponding rational function field. The transpose of any matrix S with elements in $\mathfrak{S}$ will be denoted by S' and we define the one-rowed matrices $x = (x_1, \dots, x_n)$, $u = (u_1, \dots, u_m)$. Then if A is any n -rowed square matrix with elements in $\mathfrak{F}$, $f(x) = xAx'$ is a quadratic form in $x_1, \dots, x_n$, while if B_1 is an m -rowed square matrix, $g(u) = uB_1u'$ is a second quadratic form. The general Hurwitz problem is then that of determining under what conditions on $f(x)$ and $g(u)$ there exist quantities $\gamma_{ik}^{(j)}$ in $\mathfrak{F}$ such that

$$(1) \quad f(x)g(u) = f(z)$$

where $z = (z_1, \dots, z_n)$ and

$$(2) \quad z_k = \sum_{i=1, \dots, n} \sum_{j=1, \dots, m} x_i \gamma_{ik}^{(j)} u_j \quad (k = 1, \dots, n).$$

If $f(x)$ and $g(u)$ are so related we shall show that $g(u)$ is a section of $f(x)$ and shall say that $f(x)$ or $g(u)$ permit *partial composition*. We say that $f(x)$ or $g(u)$ permit composition in case $f(x) = g(x)$.

In 1898 Hurwitz [1] considered the case $n = m$, $f(x) = g(x)$ and $\mathfrak{F}$ the field $\mathbb{C}$ of all complex numbers. He obtained the result that composition was possible if and only if $n = 2, 4$, or 8 . In 1919, L. E. Dickson [2] showed the relation of this composition to the existence of algebras of orders 2, 4 or 8 (the algebra of complex numbers, the quaternions and the Cayley numbers respectively) for which the norm of a product equals the product of the norms of the factors, and proved that there exists no linear algebra in more than eight units for which the norm is a sum of squares and the norm of a product equals the product of the norms of the factors.

In 1922 there appeared posthumously another paper of Hurwitz [3] in which he considered composition when $n \neq m$ over $\mathfrak{F} = \mathbb{C}$ and showed that m and n must stand in a certain relation in order that $f(x)$ shall permit partial composition. Here the matter rested for some years until the appearance of a paper by A. A. Albert [4] in which he proved the following generalization of the result of Dickson previously referred to.

¹ This paper is the essential portion of the author's doctoral dissertation, written at the University of Chicago under the direction of Professor A. A. Albert, whose kindness the author gratefully acknowledges.

THEOREM 1. *A quadratic form over an arbitrary field $\mathfrak{F}$ permits composition if and only if it is equivalent in $\mathfrak{F}$ to the norm form xx^J of an alternative algebra over $\mathfrak{F}$ with a unity quantity and an involution J such that $x + x^J$ and xx^J are in $\mathfrak{F}$. These latter norm forms are quadratic forms in 1, 2, 4 or 8 indeterminates except for the diagonal norm forms, in 2^t indeterminates, of purely inseparable fields of degree 2^t and exponent two over $\mathfrak{F}$ of characteristic two.*

In Part II we obtain a similar theorem for partial composition in the case $m \neq n$ over any field $\mathfrak{F}$ not of characteristic two. Then, in Part III, we consider composition over the real number field and, by means of representation theory, obtain results identical with those of Hurwitz for the complex case when the index of $g(y)$ is m and analogous results when the index of $g(y)$ is less than m .

II. THE NORM FORM THEORY

1. Basic concepts and preliminary normalizations.

In relating our quadratic forms to certain algebras we use the concept [see, for example, 5] of an algebra $\mathfrak{A}$ of order n over $\mathfrak{F}$ as a linear space $\mathfrak{L}$ of order n over $\mathfrak{F}$, a linear space $R(\mathfrak{A})$ of right multiplications of $\mathfrak{A}$ of order $m \leq n$ over $\mathfrak{F}$ consisting of linear transformations on $\mathfrak{L}$ and a linear mapping

$$y \rightarrow R_y \quad (y \text{ in } \mathfrak{A}, R_y \text{ in } R(\mathfrak{A}))$$

of $\mathfrak{L}$ on $R(\mathfrak{A})$. Similarly we have the concept of a left multiplication space $L(\mathfrak{A})$ and $x \cdot y = xR_y = yL_x$.

Before proceeding with a detailed discussion of our main problem, it is desirable to make certain normalizations of the composition equation (1). We first remark that Albert [4, p. 163] has shown that (1) is possible if and only if

$$\phi(\xi)\rho(\eta) = \psi(\zeta)$$

is possible for all quadratic forms $\phi(\xi)$ and $\psi(\zeta)$ equivalent to $f(x)$ and $\rho(\eta)$ equivalent to $g(u)$. It then results [4, p. 165] that we may take

$$f(x) = x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2, \quad g(u) = u_1^2 + b_2u_2^2 + \cdots + b_mu_m^2$$

$$(a_i, b_i \neq 0 \text{ in } \mathfrak{F}).$$

Write $R_j = (\gamma)_{ik}^{(j)}$, $L_i = (\rho)_{jk}^{(i)}$ for the $\gamma_{ik}^{(j)}$ of (2) and $\rho_{jk}^{(i)} = \gamma_{ik}^{(j)}$ for $j = 1, \dots, m$, $\rho_{jk}^{(i)}$ as yet arbitrary elements in $\mathfrak{F}$ for $j = m+1, \dots, n$. Then R_j and L_i are n -rowed square matrices with elements in $\mathfrak{F}$. Define, for $u = (u_1, \dots, u_m, 0, \dots, 0)$ and $x = (x_1, \dots, x_n)$,

$$R_u = R_1u_1 + \cdots + R_mu_m, \quad L_x = L_1x_1 + \cdots + L_nx_n,$$

so that, if $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ with 1 in the i^{th} column and zeros elsewhere, we have

$$R_{e_i} = R_i, L_{e_j} = L_j \quad (i = 1, \dots, m; j = 1, \dots, n).$$

Now let $\mathfrak{L}$ be the linear space of all $\xi = (\xi_1, \dots, \xi_n)$ for ξ_i in $\mathfrak{F}$ and write

$$(3) \quad \mathfrak{L} = \mathfrak{M} + \mathfrak{N}, \mathfrak{M} = \mathfrak{L}E, \mathfrak{N} = \mathfrak{L}(I - E), \quad E = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix}.$$

We are now considering the expression of $g(u)$ as $g(u) = uBu'$ where $B = \begin{pmatrix} B_1 & 0 \\ 0 & 0 \end{pmatrix}$, $EBE = EB = BE = B$, and write equation (1) as

$$(4) \quad f(x)g(u) = f(xR_u) = f(uL_x).$$

Now let $y = (\eta_1, \dots, \eta_n)$, take $u = yE$ and define a multiplication for all vectors x of $\mathfrak{L}$ and u of $\mathfrak{L}E$ by²

$$x \cdot u = xR_u = uL_x.$$

Clearly, (4) then implies

$$(5) \quad EBEf(x) = Bf(x) = EL_xAL'_xE,$$

so that, if $e = (1, 0, \dots, 0)$, $Bf(e) = B = EL_eAL'_eE$ and, since the rank of B is m , the rank q of EL_e has the property $m \leq q$. Also, we may write $L = \begin{pmatrix} L_1 & L_2 \\ L_3 & L_4 \end{pmatrix}$ where L_1 is an m -rowed square matrix, $EL_e = \begin{pmatrix} L_1 & L_2 \\ 0 & 0 \end{pmatrix}$ and $q \leq m$. Thus $q = m$ and there exists a non-singular square matrix P such that

$$(6) \quad EL_eP^{-1} = E, \quad EL_e = EP.$$

Writing (5) as

$$Bf(x) = (EL_xP^{-1})PAP'(EL_xP^{-1})',$$

and setting $x = e$ we obtain, by (6),

$$B = E(PAP')E.$$

By the result of Albert previously referred to [4, p. 163] we thus conclude that we may take $g(u)$ as a section of $f(u)$ and may now write (4) as

$$f(x)f(yE) = f(x \cdot yE).$$

Taking $m = n$ we may state

THEOREM 2. *If the quadratic forms $f(x) = a_1x_1^2 + a_2x_2^2 + \dots + a_nx_n^2$ and $g(u) = b_1u_1^2 + b_2u_2^2 + \dots + b_nu_n^2$ permit composition then $g(u)$ is equivalent to $f(x)$.*

We now take $m < n$ and wish to consider the equation

$$(7) \quad f(x)f(y) = f(x \cdot y)$$

for x in $\mathfrak{L}$ and y in $\mathfrak{M}$ defined by (3). We shall say that $f(x)$ or $f(y)$ permit partial composition if (7) is possible for x in $\mathfrak{L}$ and y in some subspace $\mathfrak{M}$ of $\mathfrak{L}$, and have seen that in such cases there is defined a product $x \cdot y = xR_y$ on $\mathfrak{L}, \mathfrak{M}$ to $\mathfrak{L}$. Since $f(x) = xAx'$, equation (7) is equivalent to $xAf(y)x' = xR_yAR'_yx'$ and hence to

$$(8) \quad R_yR'_y = f(y)I$$

for every y in $\mathfrak{M}$ where $R'_y = AR'_yA^{-1}$.

² We shall sometimes omit the dot in indicating such multiplications when no confusion can arise. Note that we have not yet defined a general multiplication $x \cdot y$.

The quantity $f(e) = 1$ and $eE = e$ so that, from (8), $R_e R_e^J = I$ and hence R_e is non-singular. But then $R_e^{-1}(R_e^J)^{-1} = I$, $(R_e^{-1}R_y)(R_e^{-1}R_y)^J = R_e^{-1}R_y R_y^J (R_e^J)^{-1} = f(y)I$ and $R_y^{(0)} = R_e^{-1}R_y$ is a solution of (8) when R_y is. Moreover, $R_e^{(0)} = R_e^{-1}R_e = I$. Hence we may assume without loss of generality that $R_e = I$.

For the matrix P defined by (6) we have $eP = eEP = eEL_e = eL_e = e \cdot e = eR_e = eI = e$ so that $e = eP = eP^{-1}$ and $eR_y = e \cdot y = yL_e = yEL_e = yEP = yP$ for all y in $\mathfrak{M}$. Also

$$(9) \quad f(yP) = f(y)$$

since $f(yP) = (yP)A(yP)' = eR_y A R_y' e' = eR_y R_y^J A e' = eA e' f(y) = f(e)f(y) = f(y)$.

We now write A as

$$A = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} = \begin{pmatrix} D_1 & 0 \\ 0 & D_4 \end{pmatrix}, \quad D_1 = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_m \end{pmatrix}.$$

From (9) we have $E(PAP')E = EAE$ and thus may take

$$A_0 = PAP' = \begin{pmatrix} D_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \quad D_1' = D_1, \quad A_3' = A_2, \quad A_4' = A_4.$$

Define $Q_1 = -A_3 D_1^{-1}$ to get

$$\begin{pmatrix} I_m & 0 \\ Q_1 & I_{n-m} \end{pmatrix} A_0 \begin{pmatrix} I_m & 0 \\ Q_1 & I_{n-m} \end{pmatrix}' = \begin{pmatrix} D_1 & 0 \\ 0 & A_5 \end{pmatrix}, \quad A_5 = Q_1 A_2 + A_4.$$

Now A_0 is non-singular and $\begin{pmatrix} I_m & 0 \\ Q_1 & I_{n-m} \end{pmatrix}$ is non-singular since it has the inverse $\begin{pmatrix} I_m & 0 \\ -Q_1 & I_{n-m} \end{pmatrix}$ so that A_5 is non-singular. Since $A_5' = A_5$ there exists a non-singular matrix Q_2 such that $Q_2 A_5 Q_2'$ is a diagonal matrix. Then if

$$Q = \begin{pmatrix} I_m & 0 \\ 0 & Q_2 \end{pmatrix} \begin{pmatrix} I_m & 0 \\ Q_1 & I_{n-m} \end{pmatrix},$$

we have

$$(10) \quad (QP)A(QP)' = D = \begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_m & & \\ & & & d_{m+1} & \\ & & & & \ddots \\ & & & & & d_n \end{pmatrix}.$$

Also $y = yQ$ for every y in $\mathfrak{M} = \mathfrak{L}E$ since $EQ = \begin{pmatrix} I_m & 0 \\ 0 & 0 \end{pmatrix} = E$

We may now define multiplication on $\mathfrak{L}$, $\mathfrak{MT}$ to $\mathfrak{L}$ by

$$(11) \quad (x, u) = xR_y = xR_u^{(0)}$$

where $T = QP$, $u = yT = yQP = yP$. Then, since $eR_y = yP$, we have $(e, u) = eR_y = yP = u$ while, since $e = eP$, $(x, e) = xR_e = x$.

From (8) and (9) we have

$$R_u^{(0)}(R_u^{(0)})^J = R_yR_y^J = f(y)I = f(yP)I = f(u)I.$$

Conversely, we have

$$R_u^{(0)}A(R_u^{(0)})' = f(u)A$$

so that

$$xR_u^{(0)}A(R_u^{(0)})'x' = f(u)xAx' = f(u)f(x)I = (x, u)A(x, u)' = f[(x, u)]I.$$

We now take a new basis $u_1, \dots, u_n$ of $\mathfrak{L}$ defined by

$$u_i = e_iT \quad (i = 1, \dots, n)$$

and extend our definition of multiplication on $\mathfrak{L}$, $\mathfrak{MT}$ to $\mathfrak{L}$ to a multiplication defined on $\mathfrak{L}$, $\mathfrak{L}$ to $\mathfrak{L}$ (although we do not as yet define such a multiplication for all elements of $\mathfrak{L}$). This we do by defining

$$(12) \quad (u_i, u_i) = -d_i e, \quad (u_i, u_j) = -(u_j, u_i) \\ (i \neq j, i, j = 2, \dots, n)$$

where $d_i = a_i$ for $i = 1, \dots, m$ and

$$(13) \quad u_1 = e_1QP = eP = e, \quad (u_i, e) = (e, u_i) = u_i \quad (i = 1, \dots, n).$$

We must, of course, show that this does not contradict the previous multiplication of the u_i defined by (11). Now (11) defines a multiplication (x, u) for $u = yP$, $y = yE$ in $\mathfrak{M}$. Thus for $u_i = e_iT$ we have already defined a multiplication (u_j, u_i) only for $i = 1, \dots, m$ since $e_iT = e_iP$ and e_i is in $\mathfrak{M}$ only for $i \leq m$. Then for $i = 1, \dots, m$ we have, by (11) and the fact that $eR_y = yP$ for y in $\mathfrak{M}$,

$$(14) \quad (u_i, u_i) = u_i e_i = e_i P \cdot e_i = eR_{e_i} R_{e_i} = eR_i^2,$$

while for $i \neq j$, $i, j = 1, \dots, m$ we have

$$(15) \quad (u_i, u_j) = e_i P R_{e_j} = eR_{e_i} R_{e_j} = eR_i R_j, \\ (u_j, u_i) = e_j P R_{e_i} = eR_{e_j} R_{e_i} = eR_j R_i.$$

Now for $y = (\eta_1, \dots, \eta_m, 0, \dots, 0)$

$$(16) \quad R_y = R_1 \eta_1 + \dots + R_m \eta_m$$

while

$$(17) \quad R_y^J = R_1^J \eta_1 + \dots + R_m^J \eta_m.$$

From (8) we have

$$(18) \quad R_y R_y' = (y_1^2 + a_2 y_2^2 + \cdots + a_m y_m^2) I.$$

Since (18) is an identity in the indeterminates $y_1, \dots, y_m$, (16) and (17) imply

$$(19) \quad R_i R_i' = a_i I \quad (i = 2, \dots, m),$$

and

$$(20) \quad R_i R_j' + R_j R_i' = 0 \quad (i \neq j, i, j = 1, \dots, m).$$

Setting $i = 1$ in (20) we have, since $R_e = R_1 = I$,

$$(21) \quad R_j' = -R_j \quad (j = 2, \dots, m)$$

so that

$$(22) \quad R_i^2 = -a_i I, R_1 = I \quad (i = 2, \dots, m)$$

and

$$(23) \quad R_i R_j = -R_j R_i \quad (i \neq j, i, j = 2, \dots, m).$$

Finally, since we have only defined multiplication by (11) for (x, u) with u in $\mathfrak{M}$, (12) involves no contradiction for $i \neq j, i, j = m+1, \dots, n$ and thus, by (14) and (15) we have shown that the definitions of multiplication given by (12) and (13) do not contradict those given by (11). Note that (13) makes e the unity quantity for $\mathfrak{L}$ under the multiplication just defined.

We may now summarize the results of this section as

LEMMA 1: Let $f(x)$ be a quadratic form permitting partial composition. Then there exists a linear space $\mathfrak{L}$ of order n over $\mathfrak{F}$ having a basis $u_1, \dots, u_n$ and with elements $x = (\xi_1, \dots, \xi_n)$ for ξ_i in $\mathfrak{F}$ such that

$$f(x) = xAx' = \xi_1^2 + a_2 \xi_2^2 + \cdots + a_n \xi_n^2.$$

Furthermore, we may define a multiplication on $\mathfrak{L}$, $\mathfrak{L}$ to $\mathfrak{L}$ having the properties that, for $u_1 = e$,

$$(24) \quad (u_i, e) = (e, u_i) = u_i \quad (i = 1, \dots, n),$$

$$(25) \quad (u_i, u_i) = -d_i e \quad (i = 2, \dots, n; d_i = a_i \text{ for } i = 2, \dots, m),$$

and

$$(26) \quad (u_i, u_j) = -(u_j, u_i) \quad (i \neq j, i, j = 2, \dots, n).$$

Moreover, there exists a non-singular matrix P such that, for $u = (\eta_1, \dots, \eta_m, 0, \dots, 0)P$,

$$f(x)f(u) = f[(x, u)].$$

Finally, for $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ with 1 in the i^{th} place and zeros elsewhere, we have

$$u_i = e_i P \quad (i = 1, \dots, m).$$

2. The basic theorem.

We now define a linear transformation J on $\mathfrak{L}$ by

$$u_1^J = u_1, \quad u_i^J = -u_i \quad (i = 2, \dots, n).$$

Then, if $w = \xi_1 u_1 + \dots + \xi_n u_n = xT$, we have $w^J = 2\xi_1 e - w$. From (11) we see that $R_{u_i}^{(0)} = R_i^{(0)} = R_i$ for $i = 1, \dots, m$. Thus equations (19)–(23) are true when the $R_i = R_{e_i}$ are replaced by the $R_i^{(0)} = R_{u_i}^{(0)}$ for $i = 1, \dots, m$. Then (21) and $R_1^J = R_1 = I$ imply

$$R_u^{(0)} + (R_u^{(0)})^J = 2\eta_1 I$$

for $u = \eta_1 u_1 + \dots + \eta_m u_m = yP$ and thus $R_{u^J}^{(0)} = R_{2\eta_1 e - u}^{(0)} = 2\eta_1 I - R_u^{(0)}$ so that $R_{u^J}^{(0)} = (R_u^{(0)})^J$. Therefore

$$(27) \quad eR_u^{(0)} R_{u^J}^{(0)} = eR_u^{(0)} (R_u^{(0)})^J = (u, u^J) = eR_y R_y^J = f(y)e = f(yP)e = f(u)e.$$

Now we may consider $\mathfrak{L}$ as

$$\mathfrak{L} = \mathfrak{M}' + \mathfrak{N}'$$

where $\mathfrak{M}'$ is spanned by $u_1, \dots, u_m$ and $\mathfrak{N}'$ by $u_{m+1}, \dots, u_n$. Thus every $w = \xi_1 u_1 + \dots + \xi_n u_n$ can be written as

$$w = u + v \quad (u \text{ in } \mathfrak{M}', v \text{ in } \mathfrak{N}')$$

with $v^J = -v$. Then

$$(28) \quad (w, w^J) = (u + v, u^J - v) = (u, u^J) + (v, u^J) - (u, v) - (v, v).$$

But, by (27), $(u, u^J) = f(u)e$ and $(v, u^J) = (\xi_{m+1} u_{m+1} + \dots + \xi_n u_n, \xi_1 u_1 - \xi_2 u_2 - \dots - \xi_m u_m) = (\xi_1 u_1 + \xi_2 u_2 + \dots + \xi_m u_m, \xi_{m+1} u_{m+1} + \dots + \xi_n u_n) = (u, v)$ by (24) and (26) while $-(v, v) = (v, -v) = (v, v^J) = (\xi_{m+1}^2 d_{m+1} + \dots + \xi_n^2 d_n)e$ by (25) and (26). Then $-(v, v) = f(v)e$ since $f(xT) = f(w) = xDx' = f(u) + f(v)$ by (26). Thus we may write (28) as

$$(w, w^J) = f(u)e + f(v)e = f(w)e.$$

Then $(xT, [xT]^J) = f(xT)e$ whence, upon replacing x by xT^{-1} , we have

$$(x, x^J) = f(x)e.$$

Now in order to complete our definition of multiplication in $\mathfrak{L}$ we must define (u_i, u_j) for $i \neq j$, $i, j = m+1, \dots, n$. For our present purpose it is unimportant as to what we define these products and we may agree to take all such products equal to zero. In the remainder of this section we shall revert to much of our original notation and state as

LEMMA 2: *There exists an algebra $\mathfrak{A}$ with a linear subspace $\mathfrak{M}$ over $\mathfrak{F}$, a unity quantity e and a linear transformation J over $\mathfrak{F}$ such that*

$$(29) \quad x + x^J = et(x), \quad xx^J = ef(x)$$

where $t(x)$ is a linear form and $f(x)$ is our quadratic form, with matrix A , in the coordinates $\xi_1, \dots, \xi_n$ of $x = (\xi_1, \dots, \xi_n)$. Also, for u in $\mathfrak{M}$ we have

$$(30) \quad R_u J = R_u^J = AR_u' A^{-1}$$

where R_u is defined by $xu = xR_u$ and

$$(31) \quad R_u R_u J = f(u)I.$$

Furthermore, (31) is equivalent to the partial alternative law³

$$(32) \quad x(uu) = (xu)u$$

holding for all x of $\mathfrak{X}$ and u of $\mathfrak{M}$. Finally, we have⁴

$$(33) \quad f(x)f(u) = f(xu),$$

which is equivalent to (31).

From our previous discussion it is evident that we have only to show the equivalence of (31) to (32) and (33). Now (31) implies $xR_u R_u J = xf(u)$ so $(xu)u^J = x(uu^J)$ by (29). But then $(xu)[et(u) - u] = (xu)t(u) - (xu)u$ while $x(uu^J) = x\{u[et(u) - u]\} = (xu)t(u) - x(uu)$ so that the equivalence of (31) and (32) follows. Finally, if (31) holds, $R_u A R_u' = f(u)A$, $xR_u A (xR_u)' = xAx'f(u) = (xu)A(xu)'$ so that (33) follows. Conversely, it is clear that (33) implies (31).

We may now state the main result of this section as

THEOREM 3. *Let $\mathfrak{A}$ be an algebra over $\mathfrak{F}$ with a subspace $\mathfrak{M}$ and elements $x = (\xi_1, \dots, \xi_n)$ for ξ_i in $\mathfrak{F}$ such that the partial alternative law*

$$x(uu) = (xu)u$$

holds for every x of $\mathfrak{A}$ and u of $\mathfrak{M}$. Furthermore, let $\mathfrak{A}$ possess a linear transformation J on $\mathfrak{F}$ and a unity quantity e in $\mathfrak{M}$ such that

$$x + x^J = et(x), \quad xx^J = ef(x)$$

for every x of $\mathfrak{X}$, where $t(x)$ is a linear trace form and $f(x)$ is a quadratic form in the coordinates of x . Finally, let A be a non-singular matrix such that, for $x = (\xi_1, \dots, \xi_n)$,

$$f(x) = xAx'$$

³ An alternative algebra $\mathfrak{A}$ is one in which the right hand alternative law $x(yy) = (xy)y$ and the left hand alternative law $(yy)x = y(yx)$ hold for all x and y of $\mathfrak{A}$. Thus our algebra satisfies a partial right hand alternative law.

⁴ Note that our $u = yEP = (\eta_1, \dots, \eta_m, 0, \dots, 0)P$ so that the subspace of the u 's is not the subspace of the y 's that we started out with. However, by a change of basis it is clear that we can obtain $\phi(x)\phi(y) = \phi(xy)$ where $\phi(x) \cong f(x)$ and $\phi(y) = f(y)$ is the desired section. Of course in this case $\phi(x)$ will, in general, be non-diagonal.

and let A have the property that, for every u of trace zero in $\mathfrak{M}$, the quadratic forms

$$(34) \quad (xu)Ax'$$

are identically zero. Then the norm form $f(x)$ of $\mathfrak{A}$ permits the partial composition

$$f(x)f(u) = f(xu)$$

for every x of $\mathfrak{A}$ and u of $\mathfrak{M}$. Conversely, every quadratic form permitting partial composition is equivalent to the norm form of such an algebra.

In view of Lemmas 1 and 2 it is clear that our theorem will be proved if we can show the equivalence of (34) with (30). Now if $et(u) = u + u^J = 0$ and (30) holds we have $R_{-u} = -R_u = AR'_uA^{-1}$, $-R_uA = AR'_u = (R_uA)'$ so that (34) follows since $xu = xR_u$. Conversely, suppose that (34) holds. Since $\mathfrak{M}$ is a linear subspace of $\mathfrak{A}$, x and y in $\mathfrak{M}$ imply $x + y$, x^J and y^J are in $\mathfrak{M}$ and we may write any u in $\mathfrak{M}$ as $u = \frac{1}{2}(u + u^J) + \frac{1}{2}(u - u^J)$ where $u + u^J$ is J -symmetric (i.e. $[u + u^J]^J = u + u^J$) and $u - u^J$ is J -skew (i.e. $[u - u^J]^J = -(u - u^J)$). Thus we have the result that every quantity of $\mathfrak{M}$ can be expressed as the sum of a J -symmetric element of $\mathfrak{M}$ and a J -skew element of $\mathfrak{M}$. But if v in $\mathfrak{M}$ is J -symmetric we have $v + v^J = 2v = et(v)$ so that $v = \xi e$ for ξ in $\mathfrak{F}$ while if y in $\mathfrak{M}$ is J -skew we have $y + y^J = y - y = 0$ so that y has trace zero. We have thus shown that we may write every u of $\mathfrak{M}$ as $u = \xi e + y$ where $t(y) = 0$. Then (34) implies R_yA is skew-symmetric, $R_yA = -AR'_y$, $-R_y = R_{-y} = R_{y^J} = AR'_yA^{-1}$. But $R_{e^J} = R_e = I = AR'_eA^{-1}$ since $AR'_eA^{-1} = AIA^{-1}$. Our proof is then completed by noting that $R_{u^J} = R_{\xi e^J} + R_{y^J}$ and $AR'_uA^{-1} = AR'_{\xi e}A^{-1} + AR'_yA^{-1}$.

In Theorem 1, the linear transformation J was an involution while here we may state as

COROLLARY 1: The linear transformation J of Theorem 3 is an involution of $\mathfrak{A}$ if and only if the bilinear form

$$\psi(x, y) = t(xy) - f(x + y^J) + f(x) + f(y)$$

is identically zero for all x and y of $\mathfrak{A}$.

For $(x^J)^J = x$ since $x^J = et(x) - x$, $(x^J)^J = et(x) - x^J = x$ since J is a transformation over $\mathfrak{F}$. Thus we need only to determine when $(xy)^J = y^Jx^J$. Now if λ is an indeterminate over $\mathfrak{F}$ we have

$$ef(x + \lambda y^J) = (x + \lambda y^J)(x^J + \lambda y) = xx^J + \lambda^2 y y^J + \lambda(xy + y^J x^J).$$

Then

$$\lambda(xy + y^J x^J) = [f(x + \lambda y^J) - f(x) - \lambda^2 f(y)]e$$

and

$$\lambda[(xy)^J - y^J x^J] = [\lambda t(xy) - f(x + \lambda y^J) + f(x) + \lambda^2 f(y)]e$$

whence follows the desired result.

III. COMPOSITION OVER THE REAL NUMBERS.⁵

3. The general method and results.

The problem of partial composition of two quadratic forms $g(y) = \sum_{i=1}^m \beta_i y_i^2$ and $f(x) = \sum_{i=1}^n \alpha_i x_i^2 = xAx'$ is equivalent to the problem of solving the matrix equations [4, p. 165]

$$(35) \quad G_i G_i' = \beta_i I, \quad G_i G_j' + G_j G_i' = 0, \quad G_i' = A G_i' A^{-1} \\ (i \neq j; i, j = 1, \dots, m).$$

Since we may assume $\beta_1 = 1$ [4, p. 165] we may take $G_1 = I$. Following Hurwitz [3, p. 15] we set $B_i = G_{i+1}$ so that (35) is equivalent to

$$(36) \quad B_i^2 = \gamma_i I = -\beta_{i+1} I, \quad B_i B_j = -B_j B_i, \quad B_i' = -B_i \\ (i \neq j; i, j = 1, \dots, m-1).$$

Over the field of complex numbers, Hurwitz [3] solves these matrix equations by elementary means and his method can be generalized to the case when the underlying field is algebraically closed. However, while Hurwitz's method does yield some results when the underlying field is not algebraically closed, it seems to be rather difficult work to extend his method directly for a complete treatment.

It will be seen that the method and some of the results described here will apply over any field and, in particular, over any algebraic number field. However, we will consider in detail only the case when the underlying field $\mathfrak{F}$ is the field of real numbers, $\mathfrak{R}$. This method consists, briefly, of the introduction of a *spinor algebra* [see, for example, 6 and 7] $\pi(\gamma_1, \dots, \gamma_{m-1})$ with basis $p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_{m-1}^{\epsilon_{m-1}}, \epsilon_i = 0, 1$ where

$$(37) \quad p_i^2 = \gamma_i, \quad p_i p_j = -p_j p_i \quad (i \neq j, i, j = 1, \dots, m-1)$$

and the study of the structure and representations of this algebra which is equivalent to the study of the first two equations of (36). To study the last equation of (36) we have, of course, to study the involutions of π . Leaving the details of this method to the remaining sections we now state our result. Note that here, as in the proofs, n is given for the irreducible solution [3, p. 22].

THEOREM 4. *Let $g(y) = y_1^2 + y_2^2 + \dots + y_t^2 - y_{t+1}^2 - \dots - y_m^2$. Then $g(y)$ always permits partial composition over the real numbers and, if $t = m$, we have $f(x) = x_1^2 + \dots + x_n^2$ with the values of n as given by Hurwitz [3, pp. 24-25] i.e.*

- a) $m = 2r + 1, r \equiv 0 \text{ or } 3 \pmod{4}, n = 2^r,$
 - b) $m = 2r + 1, r \equiv 1 \text{ or } 2 \pmod{4}, n = 2^{r+1},$
 - c) $m = 2r + 2, r \equiv 0, 1 \text{ or } 2 \pmod{4}, n = 2^{r+1}$
- and
- d) $m = 2r + 2, r \equiv 3 \pmod{4}, n = 2^r.$

⁵ The author is indebted to the referee for valuable suggestions on this problem.

But, if $t \neq m$, $f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2$, $s = n/2$ and, if $m = 2r + 1$, $n = 2^r$ if

a) $r \equiv 0 \pmod{4}$, $t \equiv 0$ or $1 \pmod{4}$

or

b) $r \equiv 3 \pmod{4}$, $t \equiv 0$ or $3 \pmod{4}$

and otherwise $n = 2^{r+1}$.

On the other hand, if $m = 2r + 2$, $n = 2^r$ when $r \equiv 3 \pmod{4}$, $t \equiv 0 \pmod{4}$; $n = 2^{r+2}$ when

a) $r \equiv 2 \pmod{4}$, $t \equiv 1$ or $3 \pmod{4}$,

or

b) $r \equiv 0 \pmod{4}$, $t \equiv 3 \pmod{4}$

and otherwise $n = 2^{r+1}$.

In proving Theorem 4 we shall consider separately the cases $m = 2r + 1$ and $m = 2r + 2$.

4. The case $m = 2r + 1$.

We define

$$(38) \quad u_k = p_1 p_2 \cdots p_{2k-1}, \quad v_k = p_{2k-1} p_{2k} \quad (k = 1, \dots, r).$$

From (37) and (38) it is then easy to show that

$$(39) \quad u_k^2 = (-1)^{k-1} \gamma_1 \cdots \gamma_{2k-1}, \quad v_k^2 = -\gamma_{2k-1} \gamma_{2k}, \quad u_k v_k = -v_k u_k \quad (k = 1, \dots, r).$$

Hence u_k, v_k generate a generalized quaternion algebra $\mathfrak{Q}_k = ((-1)^{k-1} \gamma_1 \cdots \gamma_{2k-1}, -\gamma_{2k-1} \gamma_{2k})$ and it is easy to see that

$$(40) \quad \pi(\gamma_1, \dots, \gamma_{2r}) = \mathfrak{Q}_1 \times \mathfrak{Q}_2 \times \cdots \times \mathfrak{Q}_r.$$

Thus π is a direct product of generalized quaternion algebras and hence is central simple. Any representation of π is completely reducible and there is only one irreducible representation in the sense of similarity [8, pp. 93-94]. If $\pi = \mathfrak{F}_s \times \mathfrak{D}$ where $\mathfrak{D}$ is a division algebra of order d_0^2 , the number, n_0 , of rows in the irreducible representation of π is $d_0^2 s$ [8, p. 107]. Since the order of π is $d_0^2 s^2 = 2^{2r}$, $n_0 = d_0 2^r$. The size, n , of the matrices of any representation is, of course, a multiple of n_0 .

This gives a basis for a discussion of the first two equations in (36). To discuss the last equation in (36) we observe that there is an involution J_0 in π that sends p_i into $-p_i$ and we let J be the involution $X \rightarrow AX'A^{-1}$ in $\mathfrak{F}_n$. Clearly, J_0 induces an involution in $\mathfrak{B}$, the algebra of representing matrices of π , and this induced involution can be extended to the involution J in $\mathfrak{F}_n$.

If we now take $g(y) = y_1^2 + \cdots + y_t^2 - y_{t+1}^2 - \cdots - y_m^2$ we will find that the algebras, $\mathfrak{Q}_k$, of (40) are of the following types—the number of each type depending, of course, on r and t (see Table I below).

1. Those in which $u_k^2 = v_k^2 = -1$. These are division algebras and will be designated by $\mathfrak{D}_k$.

2. Those in which $u_k^2 = 1, v_k^2 = -1$. These are total matrix algebras and will be designated by $\mathfrak{M}_k$.

3. When t is even, those for which $u_{t/2}^2 = v_{t/2}^2 = 1$. These are also total matrix algebras and will be designated by $\mathfrak{M}_{t/2}$.

4. When t is even, those for which $u_{t/2}^2 = -1, v_{t/2}^2 = 1$. These are also total matrix algebras and will be designated by $\mathfrak{M}_{t/2}^*$.

Our analysis will depend very largely on the following numbers:

1. n_0 = number of rows in the irreducible representation of π ;

2. d = total number of factors $\mathfrak{D}_k$ in (40);

3. d_1 = number of factors $\mathfrak{D}_k$ in (40) with k odd;

4. $d_2 = d - d_1$ = number of factors $\mathfrak{D}_k$ in (40) with k even;

5. m_0 = number of factors $\mathfrak{M}_k$ in (40) with k odd;

6. m_1 = number of factors (0 or 1) $\mathfrak{M}_{t/2}$ in (40);

7. m_2 = number of factors (0 or 1) $\mathfrak{M}_{t/2}^*$ in (40).

The constants d, d_1, m_0, m_1 and m_2 may now be calculated from (39) and are listed below in Table I for the various cases.

TABLE I

	d	d_1	m_0	m_1	m_2
A. r is odd					
1. $t \equiv 1 \pmod{4}$	$\frac{r-1}{2}$	$\frac{t-1}{4}$	$d - d_1 + 1$	0	0
2. $t \equiv 3 \pmod{4}$	$\frac{r+1}{2}$	$\frac{t+1}{4}$	$d - d_1$	0	0
3. $t \equiv 0 \pmod{4}$	$\frac{r+1}{2}$	$\frac{r+1}{2}$	0	1	0
4. $t \equiv 2 \pmod{4}$	$\frac{r-1}{2}$	$\frac{r-1}{2}$	0	0	1
B. r is even					
1. $t \equiv 1 \pmod{4}$	$\frac{r}{2}$	$\frac{t+1}{4}$	$d - d_1$	0	0
2. $t \equiv 3 \pmod{4}$	$\frac{r+2}{2}$	$\frac{t+1}{4}$	$d - d_1 - 1$	0	0
3. $t \equiv 0 \pmod{4}$	$\frac{r}{2}$	$\frac{r}{2}$	0	1	0
4. $t \equiv 2 \pmod{4}$	$\frac{r-2}{2}$	$\frac{r-2}{2}$	0	0	1

It should be noted that the entries $\frac{t-1}{4}$ and $\frac{t+1}{4}$ do not imply any restrictions on t . For, $\frac{t-1}{4}$ occurs only when $t \equiv 1 \pmod{4}$, $t = 1, 5, \dots$ for which values $\frac{t-1}{4}$ is well defined and similarly for $\frac{t+1}{4}$. Also the entry $\frac{r-2}{2}$ in B4 does not imply any restrictions on r since, when $t \equiv 2 \pmod{4}$, $t \geq 2$ and r could not be zero in this case. Finally, we may assume $t \neq 0$ by [4, p. 165].

Now since each direct product $\mathfrak{D}_i \times \mathfrak{D}_j$ is a total matrix algebra we have

LEMMA 3: $n_0 = 2^r$ or 2^{r+1} according as d is even or odd.

We now consider the representations of the factors of (40). These may be taken as follows:

$$(41) \quad \text{In } \mathfrak{D}_k, u_k = \begin{pmatrix} 0 & 1 \\ -1 & 0 & & \\ & & 0 & -1 \\ & & 1 & 0 \end{pmatrix}, \quad v_k = \begin{pmatrix} & & & 1 & 0 \\ & & & 0 & 1 \\ -1 & & 0 & & \\ 0 & -1 & & & \end{pmatrix};$$

$$(42) \quad \text{In } \mathfrak{D}_k \times \mathfrak{D}_j, u_k, v_k \text{ as in (41); } u_j = \begin{pmatrix} & & & 1 \\ & & 1 & \\ & -1 & & \\ -1 & & & \end{pmatrix},$$

$$v_j = \begin{pmatrix} & & & 1 & 0 \\ & & & 0 & -1 \\ -1 & & 0 & & \\ 0 & 1 & & & \end{pmatrix};$$

$$(43) \quad \text{In } \mathfrak{M}_j, u_j = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad v_j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

$$(44) \quad \text{In } \overline{\mathfrak{M}}_{t/2}, u_{t/2} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad v_{t/2} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

$$(45) \quad \text{In } \mathfrak{M}_{t/2}^*, u_{t/2} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad v_{t/2} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Now it is easy to verify that

$$u_k^{J_0} = (-1)^k u_k, \quad v_k^{J_0} = -v_k$$

and we now list S_k for

$$u_k^{J_0} = S_k u'_k S_k^{-1}, \quad v_k^{J_0} = S_k v'_k S_k^{-1}$$

in the various cases.

$$(46) \quad \text{In } \mathfrak{D}_k \times \mathfrak{D}_{k+2} \text{ or } \mathfrak{D}_k, k \text{ odd, } S_k = I_4.$$

$$(47) \quad \text{In } \mathfrak{D}_k \times \mathfrak{D}_{k+2} \text{ or } \mathfrak{D}_k, k \text{ even, } S_k = \text{diag } \{1, -1, 1, -1\}.$$

$$(48) \quad \text{In } \mathfrak{D}_k \times \mathfrak{D}_j, k \text{ odd, } j \text{ even, } S_k = \begin{pmatrix} & 1 & 0 \\ & 0 & -1 \\ -1 & 0 & \\ 0 & 1 & \end{pmatrix}.$$

$$(49) \quad \text{In } \mathfrak{M}_k, k \text{ even, } S_k = I_2.$$

$$(50) \quad \text{In } \mathfrak{M}_k, k \text{ odd, } S_k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

$$(51) \quad \text{In } \overline{\mathfrak{M}}_{t/2}, t/2 \text{ even, } S_{t/2} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$$(52) \quad \text{In } \mathfrak{M}_{t/2}^*, t/2 \text{ odd, } S_{t/2} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

We note that, by Table I, (51) and (52) cover all cases of $\overline{\mathfrak{M}}_{t/2}$ and $\mathfrak{M}_{t/2}^*$.

We now consider the involution J_0 on π where $X \rightarrow X^{J_0} = SX'S^{-1}$ for S the direct product of matrices given in (46)–(53). Any representation of π can be taken to have the form

$$X \rightarrow \text{diag } \{X, \dots, X\} = X \times I_h$$

where

$$X \in \pi = \mathfrak{F}_{2^r} \text{ if } d \text{ is even, } X \in \pi = \mathfrak{F}_{2^{r-1}} \times \mathfrak{D}_k \text{ if } d \text{ is odd.}$$

In the two respective cases J_0 can be extended to the involution $X_h \rightarrow TX_hT^{-1}$ in $\mathfrak{F}_{h2^r}$ or $\mathfrak{F}_{h2^{r-1}} \times \mathfrak{D}_k$ where $T = S_h$. If E is any matrix such that $EB'_iE^{-1} = -B_i$, $E = TV$ where V commutes with all the B_i . Since the B_i generate the algebra of matrices of the form X_h ,

$$(53) \quad V = I_{2^r} \times R, R \in \mathfrak{F}_h$$

if d is even while

$$(54) \quad V = I_{2^{r-1}} \times P \times R, \quad R \in \mathfrak{F}_h, \quad P = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & a_4 & -a_3 \\ -a_3 & -a_4 & a_1 & a_2 \\ -a_4 & a_3 & -a_2 & a_1 \end{pmatrix}.$$

Thus, since $E' = E$, we must have

$$(55) \quad (S \times R)' = S \times R$$

if d is even and, if $P_2 = I_{2^{r-1}}XP$,

$$(56) \quad (SP_2 \times R)' = SP_2 \times R$$

if d is odd.

Let E be cogredient to the diagonal matrix D where the quadratic form $x Dx'$ has index $n - i$ and let p be the number of terms of the form (48) appearing in S . Clearly, $p = 1$ if d is even and d_1 and t are odd and otherwise $p = 0$.

Our problem is to determine i and n for the various cases and we begin by assuming $t \neq m$.

We consider first the case when t is odd and d is even. Then the factors of S are given by (46)–(50). If $p + m_0$ is even, $S' = S$, $R' = R$, $n = 2^r$, $i = n/2$. For, E is an n -rowed matrix which is the direct product of matrices I_2 , I_4 , $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\text{diag } \{1, -1, 1, -1\}$ and, if p is odd,

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

But these matrices are cogredient to I_2 , I_4 , $\text{diag } \{I_2, -I_2\}$ or $\text{diag } \{I_4, -I_4\}$ and, if $t \neq m$, at least one non-identity matrix appears as a factor. Clearly, such a direct product must be cogredient to $\text{diag } \{I_{n/2}, -I_{n/2}\}$. On the other hand, if $p + m_0$ is odd, $S' = -S$, $R' = -R$, $n = 2^{r+1}$ and $i = n/2$.

Suppose now that d and t are both odd. Then the factors of S are (46), (47), (49) and (50) and $n_0 = 2^{r+1}$. If $S' = S$ we take $R' = R$, $P = a_1 I_4$, $n = 2^{r+1}$ and a similar argument to that given above shows that $i = n/2$. But if $S' = -S$ (which occurs if and only if m_0 is odd), (56) becomes $-P'_2 S \times R = SP_2 \times R$. To obtain a minimal value for n we wish to take $R' = R$ so that we must then have $-P'_2 S = SP_2$. It is then easily verified that this is always possible. Explicitly, we take $a_1 = a_3 = a_4 = 0$, $a_2 \neq 0$ in P if d_2 and $(m_0 - 1)/2$ are both even; $a_1 = a_2 = a_4 = 0$, $a_3 \neq 0$ in P if $(m_0 - 1)/2$ is odd and $a_1 = a_2 = a_3 = 0$, $a_4 \neq 0$ in P if d_2 is odd and $(m_0 - 1)/2$ is even. Thus we always have $n = 2^{r+1}$, $i = n/2$.

Now suppose that d and t are both even. In this case, by Table I, the factors of S are all of the form (46), (49), (51) and (52) and $n_0 = 2^r$. Of the terms (51) and (52) only (51) appears if $t \equiv 0 \pmod{4}$ while only (52) appears if $t \equiv 2 \pmod{4}$. Thus $S' = S$ or $-S$ according as $m_2 = 0$ or 1 and hence $n = 2^r$ or 2^{r+1} according as $m_2 = 0$ or 1. An argument similar to the one used above shows that $i = n/2$ in each case because of the presence of factors of the form (51) or (52) in S .

Finally, if d is odd and t is even, $n_0 = 2^{r+1}$ and we again take $P = a_1 I_4$, $R' = R$ if $S' = S$ and $a_1 = a_3 = a_4 = 0$, $a_2 \neq 0$ in P , $R' = R$ if $S' = -S$. Hence we again have $n = 2^{r+1}$ and $i = n/2$ in this case.

We have thus proved

LEMMA 4: Let $g(y) = y_1^2 + \cdots + y_t^2 - y_{t+1}^2 - \cdots - y_m^2$, $m = 2r + 1$ and $t \neq m$. Then $g(y)$ always permits partial composition and $f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2$, $s = n/2$, with $n = 2^r$ when

$$(57) \quad d \equiv p + m_0 \equiv 0 \pmod{2}, t \equiv 1 \pmod{2}$$

or

$$(58) \quad d \equiv t \equiv m_2 \equiv 0 \pmod{2}$$

and otherwise $n = 2^{r+1}$.

We now wish to know, in terms of t and r , when conditions (57) and (58) hold. By use of Table I we may obtain the result which we state as

LEMMA 5: (57) holds if and only if

a) $r \equiv t \equiv 3 \pmod{4}$

or

b) $r \equiv 0 \pmod{4}, t \equiv 1 \pmod{4}$

while (58) holds if and only if

c) $r \equiv t \equiv 0 \pmod{4}$

or

d) $r \equiv 3 \pmod{4}, t \equiv 0 \pmod{4}$.

It remains to consider the case $t = m$. Here we always have $d_2 = m_0 = m_1 = m_2 = 0$ so that $S = I_{2r}$ or I_{2r+1} with $R' = R, P = a_1 I_4$ so that E is cogredient to I_n and we always have $n = 2^{r+1}$ except when (57) or (58) hold when we have $n = 2^r$. But (57) and (58) occur only when $r = 0$ or $3 \pmod{4}$ in the case $t = m$. Hence we have

COROLLARY 2: If $g(y) = y_1^2 + \cdots + y_m^2$ where m is odd, $g(y)$ always permits partial composition over the real numbers and $f(x) = x_1^2 + \cdots + x_n^2$ where the values of n are those given by Hurwitz for partial composition over the complex numbers.

5. The case $m = 2r + 2$.

Here the element $c = p_1 p_2 \cdots p_{2r+1}$ is in the center of π and $c^2 = (-1)^r \gamma_1 \cdots \gamma_{2r+1}$. Then $\mathfrak{R}(c)$ is a direct sum of two algebras of order 1 or is a quadratic field according as $c^2 = 1$ or -1 . It should be noted that the general condition over an arbitrary field $\mathfrak{F}$ is that c^2 is or is not a perfect square in $\mathfrak{F}$ and that over the complex numbers c^2 is always a perfect square so that the case corresponding to $c^2 = -1$ here does not occur in that situation.

In the first case $\pi(\gamma_1, \cdots, \gamma_{2r+1}) = \pi_1 \oplus \pi_2$ where π_1 and π_2 are each equivalent to $\pi(\gamma_1, \cdots, \gamma_{2r})$ (except in the case when $r = 0, n \neq m = 2$ and composition is trivially possible) while, in the second case (with the same exception as noted above), $\pi(\gamma_1, \cdots, \gamma_{2r+1}) = \mathfrak{R}(c) \times \pi(\gamma_1, \cdots, \gamma_{2r})$.

We first take $c^2 = -1$. Then $\pi(\gamma_1, \cdots, \gamma_{2r+1}) = \mathfrak{R}(c) \times \pi(\gamma_1, \cdots, \gamma_{2r})$ is simple with center $\mathfrak{R}(c)$. If the number d defined for $\pi(\gamma_1, \cdots, \gamma_{2r})$ is even, $\pi(\gamma_1, \cdots, \gamma_{2r+1}) = \mathfrak{F}_s \times \mathfrak{R}(c)$ and $n_0 = 2s$. But the order of $\pi(\gamma_1, \cdots, \gamma_{2r+1})$ is $2s^2 = 2^{2r+1}$, $s = 2^r, n_0 = 2^{r+1}$. If d is odd we note that any $\mathfrak{D}_k$ is split by $\mathfrak{R}(c)$ so that we again have $\pi(\gamma_1, \cdots, \gamma_{2r+1}) = \mathfrak{F}_s \times \mathfrak{R}(c), n_0 = 2^{r+1}$. Again, as in Section 4, J_0 , defined by $p_i^{J_0} = -p_i$, induces an involution in $\mathfrak{B}$, the algebra of representing matrices of π , and this induced involution can be extended to the involution J defined by $X^J = AX'A^{-1}$ in $\mathfrak{F}_n$.

It is easy to verify that $c^{J_0} = (-1)^{r+1}c$ and $c^2 = (-1)^{r+t+1}$ and hence our assumption that $c^2 = -1$ implies that either r and t are both even or both odd. Suppose first that r and t are both odd so that $c^{J_0} = c$. Then our representation for $\mathfrak{R}(c)$ may be taken as given by

$$c = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Now our analysis of Section 4 of the two different cases $S' = S$ and $S' = -S$ arising from the fact that $E' = E$ does not occur here as E is not necessarily congruent to A but may be congruent to a multiple of A by a quantity in the center, $\mathfrak{R}(c)$, of π . Hence we may have either $E' = E$ or $E' = -E$ since $c' = -c$ and we have $n = 2^{r+1}$, E cogredient to $\text{diag } \{I_{n/2}, -I_{n/2}\}$ when $t \neq m$ and E cogredient to I_n when $t = m$.

The case when t and r are both even presents no new difficulties and we obtain

LEMMA 6: *If r and t are both even or both odd and $m = 2r + 2$, $g(y) = y_1^2 + \cdots + y_t^2 - y_{t+1}^2 - \cdots - y_m^2$ always permits partial composition and $f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2$, $s = n/2$ if $t \neq m$, $f(x) = x_1^2 + \cdots + x_n^2$ if $t = m$ with $n = 2^{r+1}$.*

There remains, finally, the case when $c^2 = (-1)^{r+t-1} = 1$. Then $\pi(\gamma_1, \cdots, \gamma_{2r+1}) = \pi(\gamma_1, \cdots, \gamma_{2r}) \oplus \pi(\gamma_1, \cdots, \gamma_{2r})$. While we have two inequivalent representations Λ_1 and Λ_2 in this case, every representing algebra is equivalent to $\pi(\gamma_1, \cdots, \gamma_{2r})$ [8, p. 120] and the most general representation is $X \rightarrow \text{diag } \{A_1, A_2, A_1, A_2, \cdots\}$ where $X \rightarrow A_1$ under Λ_1 and $X \rightarrow A_2$ under Λ_2 . Now if r is odd so that $c^{j_0} = c$ we may use for the representation of lowest order $X \rightarrow A_1$. Then, since $r + t - 1$ must be even, t must be even and our results are obtained from section 4 so that we have

LEMMA 7: *If $m = 2r + 2$ where r is odd and t is even, $g(y)$ always permits partial composition and $f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2$, $s = n/2$ when $t \neq m$ and $f(x) = x_1^2 + \cdots + x_n^2$ when $t = m$. Here $n = 2^r$ when $r \equiv 3 \pmod{4}$, $t \equiv 0 \pmod{4}$ and otherwise $n = 2^{r+1}$.*

Note that, when $t = m$, $n = 2^r$ when $r \equiv 3 \pmod{4}$ and otherwise $n = 2^{r+1}$. That is, our results again agree with those of Hurwitz for the complex case.

But now if r is even so that $c^{j_0} = -c$ we must use, for the representation of lowest order $X \rightarrow \text{diag } \{A_1, -A_1\}$ where $c = \begin{pmatrix} I_s & \\ & -I_s \end{pmatrix}$ and $c^{j_0} = \begin{pmatrix} 0 & I_s \\ -I_s & 0 \end{pmatrix} c' \begin{pmatrix} 0 & I_s \\ -I_s & 0 \end{pmatrix}^{-1}$. Noting that our minimal representations are now twice the size of the corresponding representations in Section 4 and that t odd means that $t \neq m$ we have

LEMMA 8: *If $m = 2r + 1$, r is even and t is odd, $g(y)$ always permits partial composition and $f(x) = x_1^2 + \cdots + x_s^2 - x_{s+1}^2 - \cdots - x_n^2$, $s = n/2$, with $n = 2^{r+1}$ when $r \equiv 0 \pmod{4}$, $t \equiv 1 \pmod{4}$ and otherwise $n = 2^{r+2}$.*

6. Summary.

Our proof of Theorem 4 is now made by combining the results of Corollaries 2 and 3 and Lemmas 5 through 8. We may further note that this method enables us to find z in (1) and (2) explicitly. Finally let us briefly observe that our results for composition over the real numbers differ from the results of Hurwitz over the complex numbers because of the existence of quaternion division algebras and the existence of real numbers which are not perfect squares

over the real numbers. These situations do not, of course, arise over the complex numbers.

MONTANA STATE UNIVERSITY.

BIBLIOGRAPHY

- [1] HURWITZ, A. *Über die Komposition der quadratischen Formen von beliebig vielen Variablen*. Göttingen Nachrichten (1898), pp. 309-316.
- [2] DICKSON, L. E. *On quaternions and their generalizations and the history of the eight square theorem*. Annals of Math. 20 (1919), pp. 155-171.
- [3] HURWITZ, A. *Über die Komposition der quadratischen Formen*. Math. Annalen 88 (1922), pp. 1-25.
- [4] ALBERT, A. A. *Quadratic forms permitting composition*. Annals of Math. 43 (1942), pp. 161-177.
- [5] ———. *Non-associative algebras I*. Annals of Math. 43 (1942), pp. 685-707.
- [6] CLIFFORD, W. K. *Applications of Grassmann's extensive algebra*. Am. Journ. of Math. 1 (1878), pp. 350-358.
- [7] WITT, E. *Theorie der quadratischen Formen in beliebigen Körpern*. Journ. für die reine und angewandte Math. 176 (1937), pp. 31-44.
- [8] ALBERT, A. A. *Structure of Algebras*, American Math. Soc., New York, 1939.

